



9111-14

## DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

6 CFR Part 5

[Docket No. DHS-2018-0045]

**Privacy Act of 1974:** Implementation of Exemptions; Department of Homeland Security

Department of Homeland Security (DHS)/U.S. Customs and Border Protection (CBP)-

009 Electronic System for Travel Authorization (ESTA) System of Records

**AGENCY:** Department of Homeland Security.

**ACTION:** Notice of proposed rulemaking.

**SUMMARY:** The Department of Homeland Security (DHS) is giving concurrent notice of a reissued system of records pursuant to the Privacy Act of 1974 for the “Department of Homeland Security/U.S. Customs and Border Protection (CBP)-009 Electronic System for Travel Authorization (ESTA) System of Records and this proposed rulemaking.

DHS/CBP previously issued a Final Rule to exempt this system of records from certain provisions of the Privacy Act on August 31, 2009, and codified in the Code of Federal Regulations. This Final Rule remains in effect until a new Final Rule becomes effective.

DHS/CBP is reissuing a Notice of Proposed Rulemaking to expand the applicability of the previously issued exemptions from the Privacy Act to account for the expanded categories of individuals and record source categories described in the concurrently issued SORN.

**DATES:** Comments must be received on or before [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].

**ADDRESSES:** You may submit comments, identified by docket number DHS-2018-0045, by one of the following methods:

- Federal e-Rulemaking Portal: <http://www.regulations.gov>. Follow the instructions for submitting comments.
- Fax: 202-343-4010.
- Mail: Jonathan R. Cantor, Acting Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, D.C. 20528.

**Instructions:** All submissions received must include the agency name and docket number for this notice. All comments received will be posted without change to <http://www.regulations.gov>, including any personal information provided.

**Docket:** For access to the docket to read background documents or comments received, go to <http://www.regulations.gov>.

**FOR FURTHER INFORMATION CONTACT:** For general questions please contact:

Debra L. Danisek, (202) 344-1610, [Privacy.CBP@cbp.dhs.gov](mailto:Privacy.CBP@cbp.dhs.gov), CBP Privacy Officer, Privacy and Diversity Office, 1300 Pennsylvania Ave. N.W., Washington, DC 20229.

For privacy issues please contact: Jonathan R. Cantor, (202-343-1717),

[Privacy@hq.dhs.gov](mailto:Privacy@hq.dhs.gov), Acting Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, D.C. 20528.

**SUPPLEMENTARY INFORMATION:**

I. Background:

In accordance with the Privacy Act of 1974, 5 U.S.C. 552a, DHS/CBP proposes to concurrently modify the DHS System of Records titled, “DHS/CBP-009 Electronic System for Travel Authorization (ESTA) System of Records” and issue this notice of

proposed rulemaking to exempt portions of the system of records from one or more provision of the Privacy Act because of criminal, civil, and administrative enforcement requirements. This system of records notice (SORN) describes DHS/CBP's collection and maintenance of records that pertain to eligible international travelers who wish to travel to the United States under the Visa Waiver Program (VWP) and have applied for an ESTA travel authorization and persons whose information is provided in response to an ESTA application or Form I-94W questions. DHS/CBP developed ESTA, a web-based system, in 2008 to determine the eligibility of foreign nationals to travel to the United States under the VWP. Using the ESTA website, applicants submit biographic information and answer questions that permit DHS to determine eligibility for travel under the VWP, including whether the applicant poses a law enforcement or security risk.

DHS/CBP vets the ESTA applicant's information against selected DHS and other Federal agency databases to enhance DHS's ability to determine whether the applicant poses a security risk to the United States or is otherwise eligible to travel to and enter the United States under the VWP. The ESTA eligibility determination is made prior to an alien arriving for inspection in the United States. All ESTA vetting results and derogatory information are stored in the Automated Targeting System (ATS), and covered by the ATS SORN, DHS/CBP-006 Automated Targeting System, 77 FR 30297 (May 22, 2012). Further, as explained in the concurrent notice of the updated ESTA SORN, DHS/CBP is expanding the categories of individuals to clarify the use of ESTA at all ports of entry. In addition, DHS/CBP has modified the ESTA SORN to clarify and expand several previously issued routine uses. Thus, to account for the expanded categories of individuals, record source categories and routine uses described in the concurrently

issued SORN, and to clarify that this system contains records or information recompiled from or created from information contained in other systems of records that are exempt from certain provision of the Privacy Act, DHS/CBP is reissuing a Notice of Proposed Rulemaking (NPRM) to expand the applicability of the previously issued exemptions from the Privacy Act.

Additionally, this new NPRM makes clear that this system could cover law enforcement and other derogatory records or information recompiled from or created from information contained in other systems of records that are exempt from certain provisions of the Privacy Act. These records are exempt from 5 U.S.C. 552a(c)(3) and (4); (d)(1), (2), (3), and (4); (e)(1), (2), (3), (4)(G) through (I), (5), and (8); (f); and (g) of the Privacy Act of 1974, as amended, pursuant 5 U.S.C. 552a(j)(2). Additionally, the Secretary of Homeland Security has exempted this system from the following provisions of the Privacy Act, pursuant to 5 U.S.C. 552a (k)(1) and (k)(2): 5 U.S.C. 552a(c)(3); (d)(1), (d)(2), (d)(3), and (d)(4); (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I); and (f). Such exempt records or information may be law enforcement or national security investigation records, law enforcement activity and encounter records, or terrorist screening records. DHS needs these exemptions in order to protect information relating to law enforcement investigations from disclosure to subjects of investigations and others who could interfere with investigatory and law enforcement activities. Specifically, the exemptions are required to: Preclude subjects of investigations from frustrating the investigative process; avoid disclosure of investigative techniques; protect the identities and physical safety of confidential informants and of law enforcement personnel; ensure DHS's and other federal agencies' ability to obtain information from third parties and other sources;

protect the privacy of third parties; and safeguard sensitive information.

Despite the exemptions taken on this system of records, DHS/CBP is not taking any exemption from subsection (d) with respect to information maintained in the system as it relates to data submitted by or on behalf of a person who travels to visit the United States and crosses the border, nor shall an exemption be asserted with respect to the resulting determination (authorized to travel, pending, or not authorized to travel).

However, pursuant to 5 U.S.C. 552a(j)(2), DHS/CBP plans to exempt such information in this system from sections (c)(3), (e)(8), and (g) of the Privacy Act of 1974, as amended, as is necessary and appropriate to protect this information. Further, DHS will claim exemption from section (c)(3) of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(k)(2) as is necessary and appropriate to protect this information. CBP will not disclose the fact that a law enforcement or intelligence agency has sought particular records because it may affect ongoing law enforcement activities. Nonetheless, DHS will examine each request on a case-by-case basis, and, after conferring with the appropriate component or agency, may waive applicable exemptions in appropriate circumstances and when it would not appear to interfere with or adversely affect the law enforcement or national security investigation.

DHS/CBP previously issued a Final Rule to exempt this system of records from certain provisions of the Privacy Act on August 31, 2009 (74 FR 45069). These exemptions remain in effect until a new Final Rule becomes effective. Once a Final Rule becomes effective, DHS will add this exemption to Appendix C to 6 CFR part 5, DHS Systems of Records Exempt from the Privacy Act.

## II. Privacy Act:

The Privacy Act embodies fair information practice principles in a statutory framework governing the means by which Federal Government agencies collect, maintain, use, and disseminate individual's records. The Privacy Act applies to information that is maintained in a "system of records." A "system of records" is a group of any records under the control of an agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. In the Privacy Act, an individual is defined to encompass U.S. citizens and lawful permanent residents. Additionally, and similarly, the Judicial Redress Act (JRA) provides a statutory right to covered persons to make requests for access and amendment to covered records, as defined by the JRA, along with judicial review for denials of such requests. In addition, the JRA prohibits disclosures of covered records, except as otherwise permitted by the Privacy Act.

The Privacy Act allows government agencies to exempt certain records from the access and amendment provisions. If an agency claims an exemption, however, it must issue a Notice of Proposed Rulemaking to make clear to the public the reasons why a particular exemption is claimed.

#### **List of Subjects in 6 CFR Part 5**

Freedom of information; Privacy.

For the reasons stated in the preamble, DHS proposes to amend Chapter I of Title 6, Code of Federal Regulations, as follows:

#### **PART 5--DISCLOSURE OF RECORDS AND INFORMATION**

1. The authority citation for part 5 is revised to read as follows:

**Authority:** 6 U.S.C. 101 et seq.; Pub. L. 107-296, 116 Stat. 2135; 5 U.S.C. 301.

2. In appendix C to part 5, revise paragraph 20 to read as follows:

Appendix C to Part 5 – DHS Systems of Records Exempt From the Privacy Act

\* \* \* \* \*

20. The Department of Homeland Security (DHS)/U.S. Customs and Border Protection (CBP)-009 Electronic System for Travel Authorization (ESTA) System of Records consists of electronic and paper records and will be used by DHS and its components. The DHS/CBP-009 Electronic System for Travel Authorization (ESTA) System of Records is a repository of information held by DHS in connection with its several and varied missions and functions, including, but not limited to the enforcement of civil and criminal laws; investigations, inquiries, and proceedings there under; national security and intelligence activities. This system of records covers information collected by, on behalf of, in support of, or in cooperation with DHS and its components and may contain personally identifiable information collected by other federal, state, local, tribal, foreign, or international government agencies. As part of the process of determining ESTA eligibility or admissibility to the United States under the Visa Waiver Program, CBP collects two types of data for which it claims different exemptions.

(a) CBP will not assert any exemption to limit an individual from accessing or amending his or her record under subsection 552a(d) with respect to information maintained in the system as it relates to data submitted by or on behalf of a person who travels to visit the United States and crosses the border, nor shall an exemption be asserted with respect to the resulting determination (approval or denial). However, pursuant to 5 U.S.C. 552a(j)(2), CBP will not disclose the fact that a law enforcement or intelligence agency has sought particular records because it may affect ongoing law

enforcement activities, and thus, the Secretary of Homeland Security has exempted such records covered by this system from sections (c)(3), (e)(8), and (g) of the Privacy Act of 1974, as amended, as is necessary and appropriate to protect this information. Further, DHS will claim exemption from section (c)(3) of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(k)(2) as is necessary and appropriate to protect this information. Exemptions from these particular subsections are justified, on a case-by-case basis to be determined at the time a request is made, for the following reasons:

- (i) From subsection (c)(3) (Accounting for Disclosures) because release of the accounting of disclosures could alert the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of that investigation and reveal investigative interest on the part of DHS as well as the recipient agency. Disclosure of the accounting would therefore present a serious impediment to law enforcement efforts and/or efforts to preserve national security. Disclosure of the accounting would also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension, which would undermine the entire investigative process.
- (ii) From subsection (e)(8) (Notice on Individuals) because compliance would interfere with DHS's ability to obtain, serve, and issue subpoenas, warrants, and other law enforcement mechanisms that may be filed under seal and could result in disclosure of investigative techniques, procedures, and evidence.
- (iii) From subsection (g) (Civil Remedies) to the extent that the system is exempt from other specific subsections of the Privacy Act.



(b) Additionally, this system contains law enforcement and other derogatory records or information recompiled from or created from information contained in other systems of records that are exempt from certain provisions of the Privacy Act. For these records or information only, the Secretary of Homeland Security, pursuant to 5 U.S.C. 552a(j)(2), has exempted this system from the following provisions of the Privacy Act: 5 U.S.C. 552a(c)(3), (c)(4); (d)(1)-(4); (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(5) and (e)(8); (f); and (g). Additionally, the Secretary of Homeland Security, pursuant to 5 U.S.C. 552a(k)(2), has exempted this system from the following provisions of the Privacy Act, 5 U.S.C. 552a(c)(3); (d)(1)-(4); (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I); and (f). Exemptions from these particular subsections are justified, on a case-by-case basis to be determined at the time a request is made, for the following reasons:

- (i) From subsection (c)(3) and (c)(4) (Accounting for Disclosures) because release of the accounting of disclosures could alert the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of that investigation and reveal investigative interest on the part of DHS as well as the recipient agency. Disclosure of the accounting would therefore present a serious impediment to law enforcement efforts and/or efforts to preserve national security. Disclosure of the accounting would also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension, which would undermine the entire investigative process.
- (ii) From subsection (d) (Access to Records) because access to the records contained in this system of records could inform the subject of an

investigation of an actual or potential criminal, civil, or regulatory violation to the existence of that investigation and reveal investigative interest on the part of DHS or another agency. Access to the records could permit the individual who is the subject of a record to impede the investigation, and to avoid detection or apprehension. From subsection (d) (Amendment to Records) because amendment of the records could interfere with ongoing investigations and law enforcement activities and would impose an unreasonable administrative burden by requiring investigations to be continually reinvestigated. In addition, permitting access and amendment to such information could disclose security-sensitive information that could be detrimental to homeland security.

- (iii) From subsection (e)(1) (Relevancy and Necessity of Information) because in the course of investigations into potential violations of federal law, the accuracy of information obtained or introduced occasionally may be unclear, or the information may not be strictly relevant or necessary to a specific investigation. In the interests of effective law enforcement, it is appropriate to retain all information that may aid in establishing patterns of unlawful activity.
- (iv) From subsection (e)(2) (Collection of Information from Individuals) because requiring that information be collected from the subject of an investigation would alert the subject to the nature or existence of the investigation, thereby interfering with that investigation and related law enforcement activities.
- (v) From subsection (e)(3) (Notice to Subjects) because providing such detailed

information could impede law enforcement by compromising the existence of a confidential investigation or reveal the identity of witnesses or confidential informants.

- (vi) From subsections (e)(4)(G), (e)(4)(H), and (e)(4)(I) (Agency Requirements) and (f) (Agency Rules), because portions of this system are exempt from the individual access provisions of subsection (d) for the reasons noted above, and therefore DHS is not required to establish requirements, rules, or procedures with respect to such access. Providing notice to individuals with respect to existence of records pertaining to them in the system of records or otherwise setting up procedures pursuant to which individuals may access and view records pertaining to themselves in the system would undermine investigative efforts and reveal the identities of witnesses, potential witnesses, and confidential informants.
- (vii) From subsection (e)(5) (Collection of Information) because with the collection of information for law enforcement purposes, it is impossible to determine in advance what information is accurate, relevant, timely, and complete. Compliance with subsection (e)(5) would preclude DHS agents from using their investigative training and exercise of good judgment to both conduct and report on investigations.
- (viii) From subsection (e)(8) (Notice on Individuals) because compliance would interfere with DHS's ability to obtain, serve, and issue subpoenas, warrants, and other law enforcement mechanisms that may be filed under seal and could result in disclosure of investigative techniques, procedures, and evidence.

- (ix) From subsection (g) (Civil Remedies) to the extent that the system is exempt from other specific subsections of the Privacy Act.

Jonathan R. Cantor  
Acting Chief Privacy Officer,  
Department of Homeland Security  
[FR Doc. 2019-13647 Filed: 6/26/2019 8:45 am; Publication Date: 6/27/2019]